White paper

Global trends in the safety of machinery

New requirements for PL and SIL

Find out more about

- Upcoming revisions to the EN ISO 13849 and IEC 62061 standards
- Effects on the topic of cybersecurity
- Changes in the field of safety-relevant software

PHOENIX CONTACT

Introduction

Those who want to respond quickly and flexibly to customer requirements are dependent on complex and decentral industrial production facilities. In this context, the topic of functional safety is of increasing importance. The trend of decentralization brings new challenges regarding the protection of people and the environment and the safety of machinery. Besides classical safety equipment such as safety door interlocking systems, emergency stop equipment, and safety switches, more and more programmable or configurable safety systems for the safeguarding of machines and systems are being used as the degree of complexity increases. The availability of production equipment should not be restricted any more than is necessary.

In 2015, an attempt was made to merge the EN ISO 13849 and IEC 62061 standards into one document. Currently, both standards are being revised separately. EN ISO 13849 is scheduled for publication at the beginning of 2023. Safety expert Carsten Gregorius, representing Phoenix Contact as a member of the standardization committees, explains which changes to expect with regard to PL and SIL: In some respects, such as safety-relevant software and cybersecurity, both standards have already become very similar.

Many other detailed changes have been incorporated resulting in overall greater consistency between the two standards. Whether this will have consequences for existing safety assessments will have to be determined on a case-by-case basis.

Read on for detailed information about the changes being made to the standards.

Contents

1 What are the changes for PL and SIL?

The safety of machines and systems necessary to protect users mainly depends on the correct application of the standards and directives. In Europe, the basis for this is the Machinery Directive, which provides standard specifications to support companies when designing safety-related machines. However, even outside the European Economic Area, many European standards are gaining importance due to their international status. In this context, the standards on functional safety also play important roles. The requirements on machine control systems are specified both in EN ISO 13849 and IEC 62061.

Besides the fundamental wish to improve the readability of the standards, the work on EN ISO 13849 was focused on a clear and unambiguous specification of the safety requirements (SRS). Moreover, the method for determining the risk level PLr, for which detailed specifications regarding the determination of the parameter P exist, will be expanded. The requirements on safety-relevant software in particular will be defined in more detail.

Overview of the most important changes to EN ISO 13849 and IEC 62061

EN ISO 13849	IEC 62061
Additional specifications for determining the parameter P (risk level PLr)	Change of the designation from "SILCL" to "SIL"*
Unambiguous specification of the safety requirements (SRS)	Consideration of low-demand applications (not yet considered in the 2021 version of the standard; will follow in a later amendment)
Precise definition of "proven components"	Adjustment of validation process on the basis of EN ISO 13849*
Adjustment of validation process on the basis of EN ISO 13849-2*	
PFH_D substitute values for inputs and outputs	Scope of application becomes independent of the technology (no longer limited to E/E/PES)*
Precise requirements on safety-relevant software	
Influence of cybersecurity on "functional safety"	
Precise definition of "diagnostic coverage" (DC)*	Examples of failure rates ($MTTF_D$), diagnostic coverage (DC) on the basis of EN ISO 13849*
Detailed information on the "common cause failure" (CCF) with regard to the influence of EMC*	Examples of the evaluation of common cause failures on the basis of EN ISO 13849*
Device types 1 to 4 (Appendix O) *	

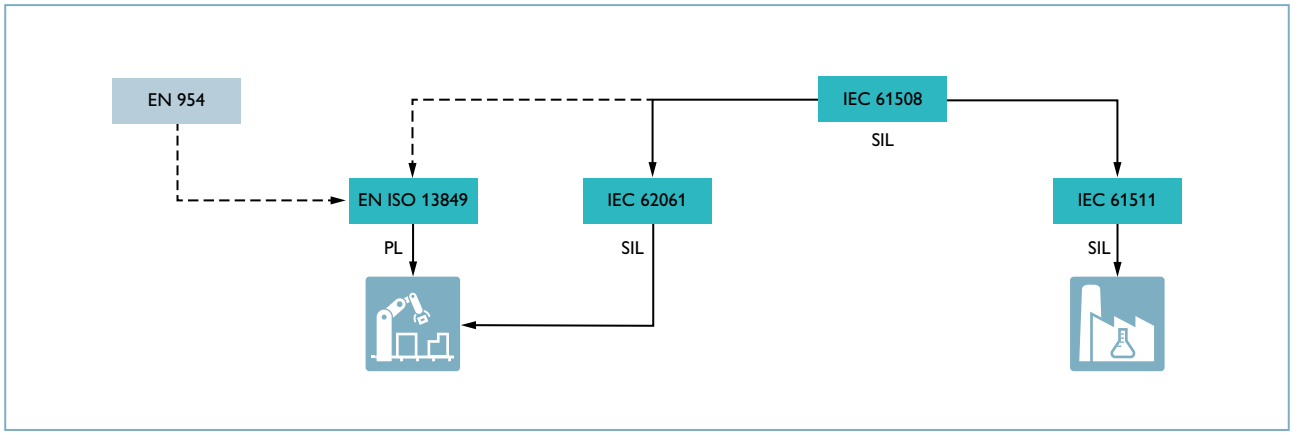
* These changes are not dealt with further in this white paper

Additional changes to EN ISO 13849 relate to clarifications of the diagnostic coverage (DC) and the definition of "proven components". The aspect of "common cause failure" (CCF) has been detailed in EN ISO 13849 with regard to EMC interference.

For reasons of consistency with IEC 61508 and other sector standards, one important change was made to IEC 62061 regarding the safety characteristic data: In the future, the concept of "SIL" will be used instead of "SILCL" (SIL claim). Moreover, the method for determining the failure rates of components, as well as the validation process, have been detailed. The parameter λ_D from the definition of failure rates of components in accordance with IEC 62061 is now related to the $MTTF_D$ [1] and $B10_D$ [2] definitions from EN ISO 13849. The validation of the safety functions must prove that the requirements on the safety-relevant parts of the control system are implemented in accordance with their defined characteristics. A new element of IEC 62061 is the well-known validation process flow chart from EN ISO 13849, part 2.

Finally, both standards address the influence of cybersecurity on "functional safety".

The requirements on machine control systems are specified both in EN ISO 13849 and IEC 62061.



The importance of EN ISO 13849 and IEC 62061

Many type-C standards refer to at least one of these standards when addressing the safe design of machinery. Both standards consider aspects from the IEC 61508 basic standard. EN ISO 13849 was developed about 20 years ago from the former EN 954, whereas IEC 62061 was developed as a sector standard for "machinery".

In parallel, IEC 61511 exists as a sector standard for the process industry, but will not be dealt with further in this document.

[1] $MTTF_D$: Mean time to dangerous failure

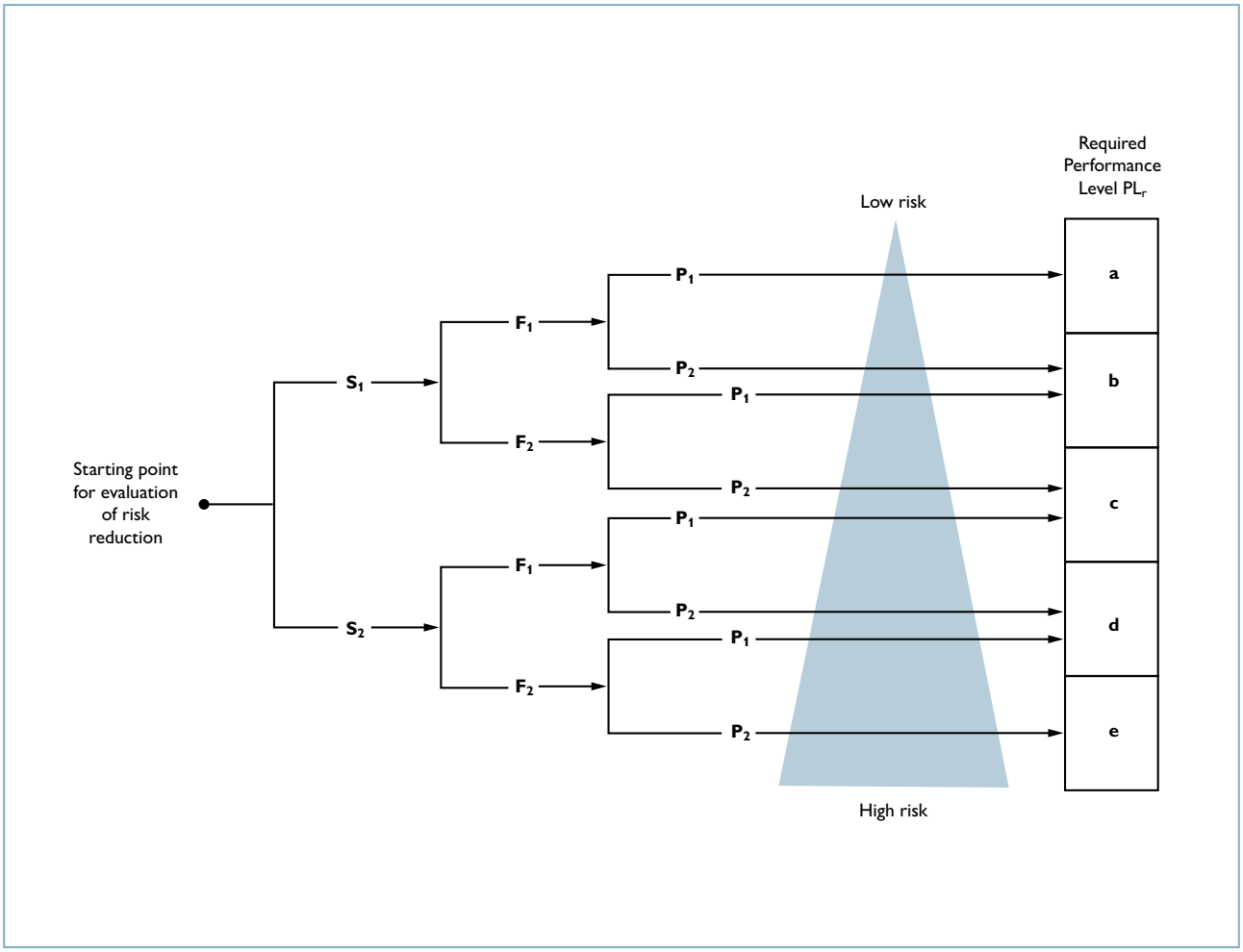
[2] $B10_D$: Mean number of switching cycles until 10% of the components fail dangerously

Determination of the required PLr in accordance with EN ISO 13849

The "required performance level (PLr)" is of essential importance in the process of risk reduction. Depending on the degree of risk, one of the five levels "a" to "e" is selected, taking into account the following parameters: S (seriousness of injury), F (frequency and/or duration of the exposure to the hazard), or P (possibility of preventing the hazard or limiting the harm).

In the past, when it came to parameter P in particular, the question of when to select P1 (possible under certain conditions) or P2 (impossible) often arose.

For determining the parameters P1 or P2, a selection guide will be provided which evaluates the aspects of qualification, velocity of hazard propagation, and complexity.



Determination of the PLr

Selection guide for determining the parameter P

Description	A	B	C
Training	Trained personnel	Untrained personnel	–
Speed of the hazardous movement	Low: e.g., <250 mm/s; time left until hazard is reached >3 s	Medium: e.g., 251 mm/s – 1000 mm/s, time left until hazard is reached <3 s	High: e.g., <1000 mm/s; time left until hazard is reached <1 s
Possibility of escaping the hazard in a specific place	>=50% of cases	<50% of cases	Not possible
Possibility to recognize the hazard	>=50% of cases	<50% of cases	Not possible
Complexity (number/duration of operator interventions)	Low degree of complexity (e.g., adjustment of collets, inserting workpieces)	High or medium degree of complexity (troubleshooting, set-up in inching mode)	–

Depending on the number of resulting classifications A, B, or C, the parameters P1 or P2 can then be specified. When the evaluation process results in at least one C or three B classifications, this leads directly to a P2 classification.

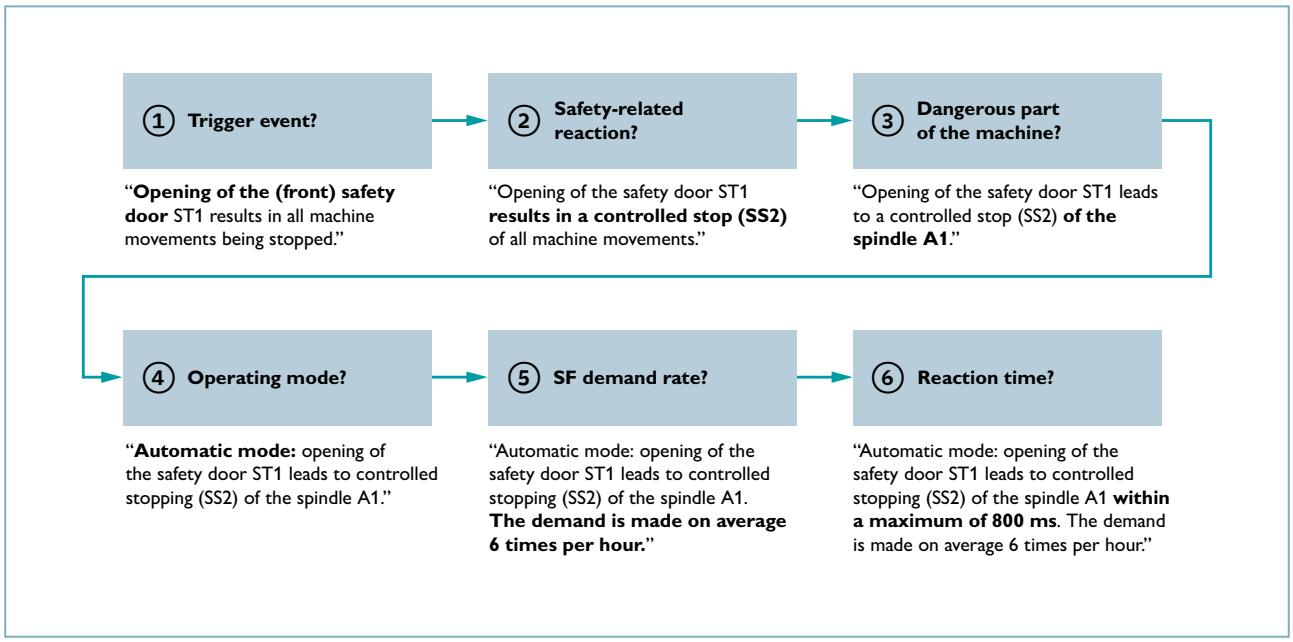
Specification of the safety function in accordance with EN ISO 13849

Critical events related to safety-relevant control systems frequently occur due to an insufficient specification. This can mean that even if all other verification steps are correctly taken, there may be only an insufficient reduction of risk in the end.

For this reason, the EN ISO 13849 standard authors have focused on the detailed description of what is known as the SRS (Safety Requirements Specification).

The following questions should provide guidance during the validation process:

1. What is the trigger event?
2. What is the safety-related response?
3. Which are the dangerous parts of the machine?
4. In which operating mode is the safety function effective?
5. How frequently is the safety function required?
6. Within what response time is the safe state reached?



Example of the procedure for the specification of a safety function

The example includes every single step needed to achieve a detailed "specification of the safety functions". This procedure allows common tools that also support this approach (e.g., SISTEMA[3]) to be used.

Proven components in accordance with EN ISO 13849

The term "proven component" is particularly relevant for the interpretation in accordance with category 1 specified in EN ISO 13849. A component is considered to be "proven" when it has already been used successfully in similar applications in the past and documented accordingly. Alternatively, such a component is considered proven if it has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications. Whether a certain component is accepted as being "proven" depends on the application and environmental influences, for example. Complex electronic components (e.g., PLC, microprocessor, and application-specific integrated circuit) cannot be considered as equivalent to "proven".

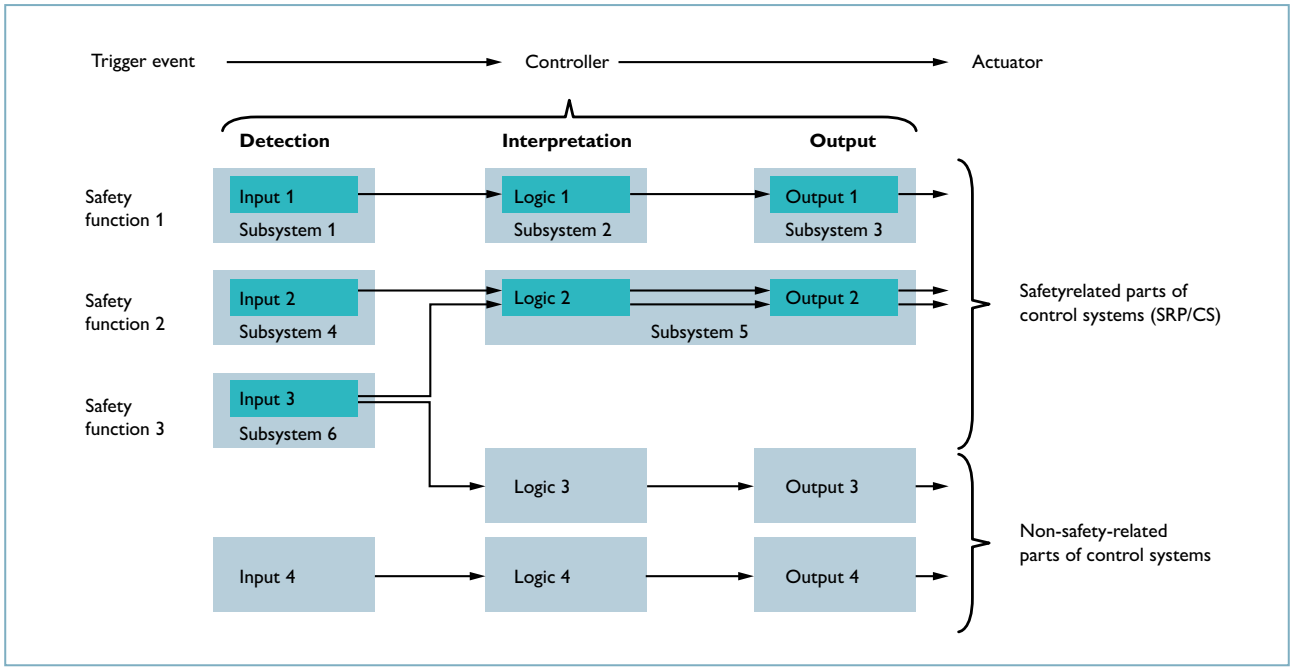
Are characteristics missing? Substitute values in accordance with EN ISO 13849

After defining the safety function (SRS) and determining the PLr in accordance with EN ISO 13849, the next step is to identify the safety-relevant parts of the control system before breaking down the safety function into "subsystems". In doing so, subsystems can be assigned to different safety functions.

[3] SISTEMA: safety of control systems on machines (Published by IFA = Institute for Occupational Health and Safety of the German Social Accident Insurance)

The next step is to determine the safety characteristics (PFH_D, service life, etc.) for each subsystem. An easy way for users is to take the values provided by the component manufacturer (e.g., safety PLC). However, some applications use standard components for which these characteristics are not available.

Until now, 10 years could be assumed for an $MTTF_D$. But in many cases that is too "conservative". In the future, for subsystems with discrete components, it will be possible to use the PFH_D substitute values from the table below when no manufacturer's information is available.



Safety functions and their assignment to subsystems

	PFHD 1/h	Category B	Category 1	Category 2	Category 3	Category 4
PL b	$5*10^{-6}$	X	O	O	O	O
PL c	$1.7*10^{-6}$	–	X*	X*	O	O
PL d	$2.9*10^{-7}$	–			X*	O
PL e	$4.7*10^{-8}$	–	–	–	–	X*

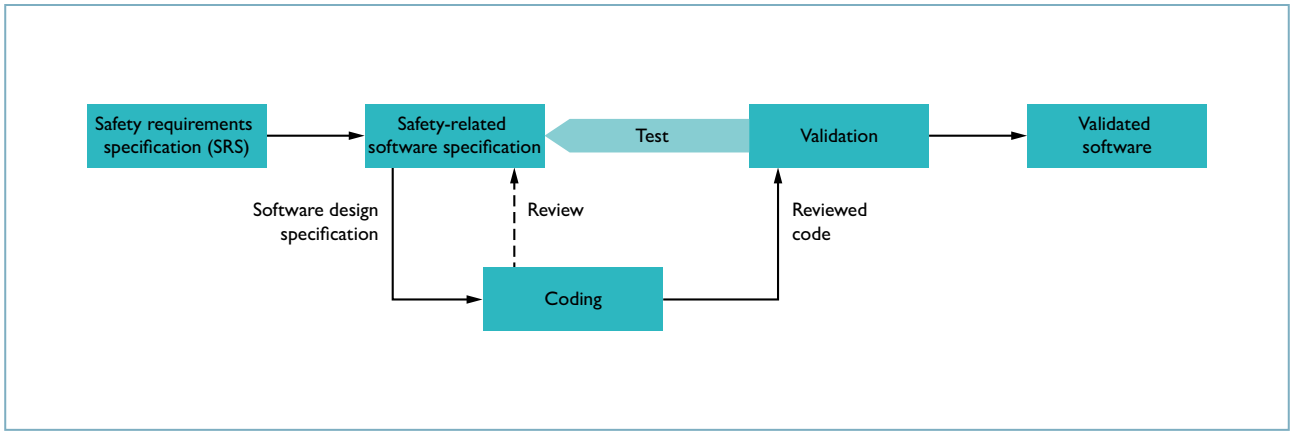
PFH_D substitute values for inputs and outputs

X: Used category is recommended. O: Used category is optional
*: Proven components and proven safety technology principles must be applied
–: Category is not permitted

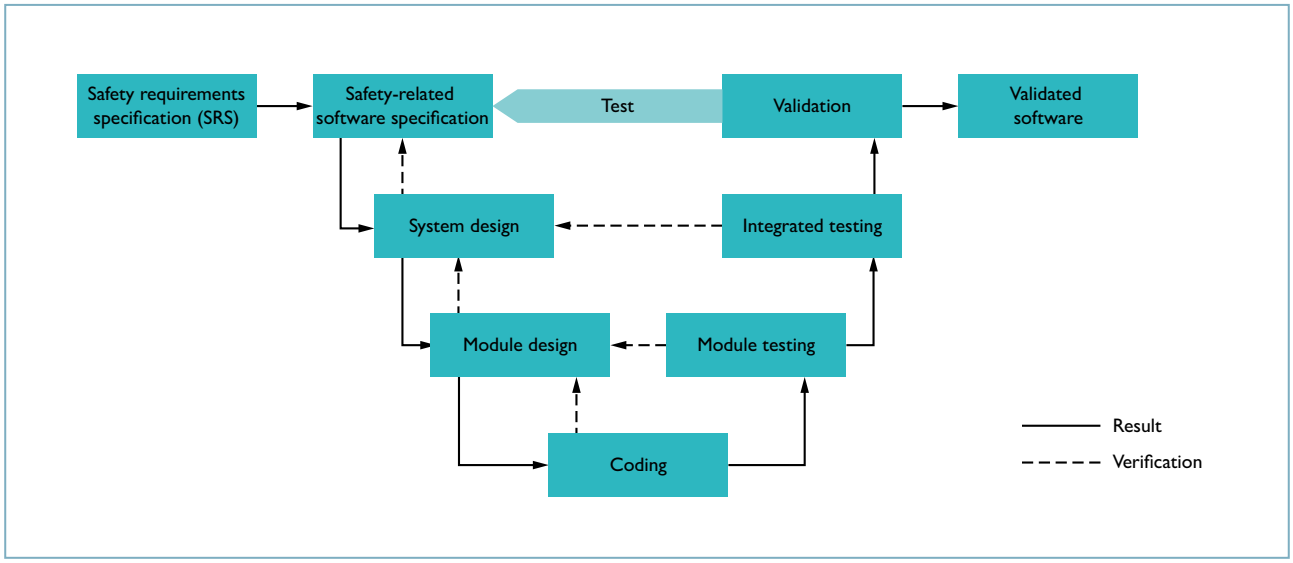
Requirements on safety-relevant software in accordance with EN ISO 13849/IEC 62061

For machine control systems, configurable or programmable systems that have already been certified in accordance with IEC 61508 are being increasingly used.

For those systems in particular as well as for systems using LVL[4] languages, significant simplifications regarding the verification and validation of safety functions can be anticipated. The existing V model, for example, has been simplified in EN ISO 13849 for this application, so that besides the SRS software, "coding" and "software testing" are the only steps remaining.



Simplified V model



V model for FVL[5] languages

[4] LVL: Limited Variability Languages = programming languages with limited variability

When FVL[5] languages, such as Ada, C, Assembler, etc., are used however, the former V model remains mandatory for the application.

Similarly, IEC 62061 defines so-called "software levels". The standard describes three levels. The first level includes the pre-designed systems described in LVL languages, for which a simplified validation method will be possible (similarly to EN ISO 13849). When the languages referred to as FVL languages are used, the verification and validation process is more comprehensive.

The table below shows the minimum levels of independence resulting from this for software level 1. Additionally, users may use the simplified V model (see EN ISO 13849).

In summary, it can be said that when using precertified systems and software blocks, significant simplification of the verification and validation process can be expected.

Software level	**Platform** (combination of hardware and software)	**Example**
1	"Predesigned" in accordance with IEC 61508 (application software that uses LVL)	Safety PLC with LVL or programmable safety relay module
2	"Predesigned" in accordance with IEC 61508 (application software that does not use LVL)	Safety PLC with FVL in accordance with IEC 62061
3	"Predesigned" in accordance with IEC 61508 (application software that does not use LVL)	Safety PLC with LVL or FVL in accordance with IEC 61508

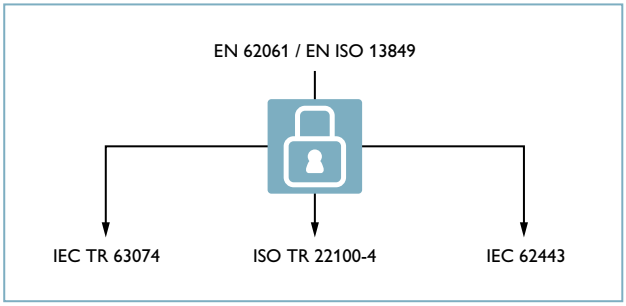
Minimum level of independence	**SIL required for the safety function**		
	1	**2**	**3**
Same person	Insufficient	Insufficient	Insufficient
Different person	Only if precertified software modules are used	Only if precertified software modules are used	Insufficient
Independent person*	Sufficient	Sufficient	Sufficient

* Depending on the company organization and expertise within the company, the requirement for an "independent person" may need to be met through the use of an external organization. Organizations that have internal organizations knowledgeable in risk assessment and the application of security-related systems may use their own resources to meet the requirements for an independent organization, provided they are independent and separated by management and other resources from those responsible for the main development.

[5] FVL: Full Variability Languages = programming languages with full variability

Influence of cybersecurity on functional safety in accordance with EN ISO 13849 / IEC 62061

In contrast to functional safety, cybersecurity protects goods from detrimental adverse affects as a result of intentional or inadvertent attacks on the availability, integrity, and confidentiality of the data. This involves the use of preventative, technical, and organizational measures.



Situation regarding standardization: Cybersecurity with functional safety

As the networking of automation systems with the IT world is becoming more and more commonplace, scenarios are likely to arise where a different approach is required, especially for safety applications. The network interfaces between office IT systems and production networks are a significant gateway for hackers. This potential risk is also reflected in the two standardization projects and will have to be considered in the future, for example by performing an IT risk assessment based on the IEC 62443 standard.

Low-demand systems for machines in accordance with IEC 62061

The scope of the Machinery Directive is, on the one hand, a very broad one in practical use. Besides classical machines, the directive covers systems such as gas and steam turbines, compressors, generators, or pumps. On the other hand, the two harmonized standards on functional safety, EN ISO 13849 and IEC 62061, have not yet addressed "low-demand applications".[6] Due to the incorrect presumption of conformity, this has led to legal uncertainty for the manufacturers of such systems. Now at least, IEC 62061 will take on this approach in a future amendment by defining PFD[7] failure limit values based on IEC 61508.

When IEC 62061 is applied correctly, low-demand applications can now also be evaluated within the scope of the Machinery Directive, claiming "presumption of conformity."

SIL	PFDavg target failure measures for low demand
1	$< 10^{-1}$
2	$< 10^{-2}$
3	$< 10^{-3}$

[6] Operating mode in which the frequency of safety function demands is no more than once per year and no more than twice the frequency of the proof test

[7] Probability of dangerous failure on demand

2 Side note: Working in a standardization committee

Experts from Phoenix Contact are members in every important standardization committee. Our customers can access this know-how either through our online sales channels or our local representatives. Safety expert Carsten Gregorius represents Phoenix Contact as a member in the national standardization committees on ISO 13849 and IEC 62061.

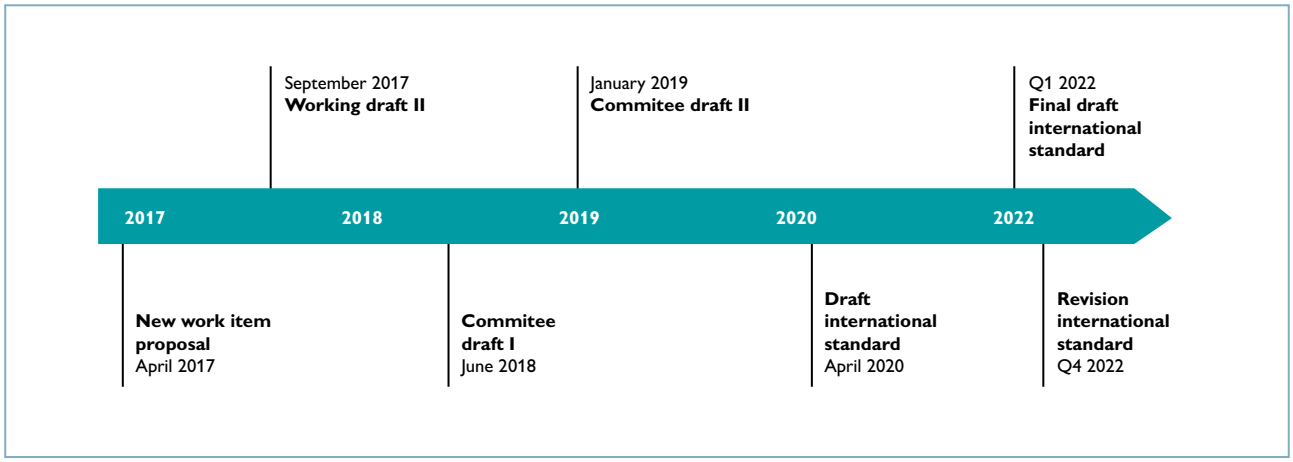
What is it like working in a standardization committee?

Before a new standardization project can start on the international level, a proposal (NWIP = new work item proposal), practically a "profile", must be prepared. When this process has been completed successfully, the project starts with the nomination of an international group of experts. This international committee now works on the actual contents. The international working group then prepares draft standards called "committee drafts" or "FDIS". These are circulated to all national standardization committees, also known as "mirror committees", for comment. In Germany, the DIN (German Institute for Standardization) often directs the work of the mirror committees.

Safety expert Carsten Gregorius from Phoenix Contact

What happens next?

In principle, everyone can submit their comments or corrections for a draft standard through the national standardization committees. This is why, depending on the standardization project and the member country, hundreds of individual comments often need to be considered. But because small and medium-sized companies in particular often don't have the time to contribute to all the different standardization committees, associations such as VDMA or ZVEI take on some of these tasks.



Schedule for the revision of EN ISO 13849

And how exactly is a new standard drawn up then?

When all comments from the national mirror committees have been returned to the international standardization group, they are incorporated into another draft. Finally, this FDIS[8] is circulated, for a final vote, to all countries eligible to vote. An FDIS is then either approved by a majority or rejected. A positive result means the new version of EN ISO 13849, as an example, can be published.

What projects will follow?

When the revision of EN ISO 13849 (part 1) has been completed, a subsequent revision step is planned where calculation models for the determination of the PFH_D will be added to Technical Report EN ISO/TR 23849. Another project will be about revising part 2 of EN ISO 13849 (validation), before parts 1 and 2 will then be merged.

[8] FDIS: Final Draft International Standard

Glossary

Common cause failure
Refers to the operational failure of different elements resulting from common single events where these failures are not consequences of each other.

Dangerous failure per hour
Probability of a dangerous failure per hour (PFHD).

Diagnostic coverage
Measurement for the effectiveness of the diagnostics represented as the ratio between the failure rate of the identified failure rates and the rate of total failures. Diagnostic coverage can either relate to the entire system or to certain components, such as sensors, logical systems, or final elements.

Harmonized standard
Harmonized standards are European standards for products listed in the official journal under a European Directive. They are part of the European Commission's "New Approach," in which essential requirements for products are defined by the standards organizations CEN and CENELEC. The harmonized standards are published in the Official Journal of the EU. Only goods and services that satisfy the essential requirements from the directives may be placed on the market. They can be identified by certificates or CE markings.

Performance level
The performance level (PL) is a qualitative classification of the individual SRP/CS (safety-related parts of control systems) with regard to the performance capability of the individual safety functions in the event of unforeseeable situations.

Contact

Book your consultation now!

Are you looking for a powerful partner for functional safety?

Phoenix Contact will provide the products, training courses, and TÜV-certified experts to help you meet the safety requirements of the Machinery Directive and the process industry. We will get you fit for the safety of people and machines.

#FitForSafety

Carsten Gregorius
Product Marketing for Safety at Phoenix Contact,
author of white paper

cgregorius@phoenixcontact.com

Further reading and links:

Funktionale Sicherheit von Maschinen –
Praktische Anwendung der DIN EN ISO 13849-1
(in German only)
Beuth-Verlag: ISBN 978-3-410-25249-8

Safety meets security –
A common strategy is required
Visit us at phoenixcontact.com/safety-meets-security

AI 04-22.002.L3